FIREWALL PROTECTION PROFILE
FREQUENTLY ASKED QUESTIONS AS OF 6/13/97

1. What is the purpose of the specification?

The firewall protection profile is a security requirements specification being prepared by the Federal Government that defines the basic needs of organizations handling unclassified information. The profile was written to comply with version 1.0 of the Common Criteria for Information Technology Security Evaluation (a.k.a. Common Criteria), a standard being developed jointly by the National Institute of Standards and Technology, the National Security Agency, and Government agencies from five other nations. As a minimal requirements specification, it fulfills multiple purposes: to serve as an example protection profile that demonstrates the suitability of the Common Criteria for non-operating systems products, to become the basis for firewall product evaluations by independent laboratories accredited to perform Common Criteria security evaluations, to be used in Government procurement activities, and to provide a suitable requirements baseline for use by industry.

2. What is the rational for the unique structure of these requirements and the use of new, unfamiliar terminology?

The structure and content of a protection profile are dictated to a large degree by the Common Criteria. A protection profile contains predefined functionality and assurance components drawn from the Common Criteria to meet stated security objectives and policy required for a class of product or system. The functionality and assurance components are requirements written in natural language (i.e., English), but done so in a manner that maintains uniformity in style and structure, and consistency in the use of security related terms. Unfortunately, the resulting text sometimes appears a bit stiff and overly full of jargon. However, this shortcoming is offset by the benefits of component reuse in other profiles, consistent interpretation by security evaluators, and the possibility for mutual recognition of evaluation results with other nations. For more information on the Common Criteria, see either http://csrc.nist.gov/nistpubs/cc/ or http://www.radium.ncsc.mil/tpep/library/ccitse/index.html.

3. How do some of the Common Criteria terms used in the specification map to more common, information technology terms?

The Common Criteria uses many specialized terms that may not make sense upon first reading. Some of the more onerous terms used in the firewall protection profile are translated below.

- Target of Evaluation (TOE) - a firewall implementation under assessment against the requirements specified in the protection profile (e.g., brand X firewall product).
- TOE Security Policy (TSP) - the security rules that define the behavior of a firewall implementation.

- TOE Security Functions (TSF) - the security mechanisms of a firewall that enforce its security policy (i.e., the TSP); formerly known as the trusted computing base under the Orange Book.
- Security Function (SF) - a portion of a firewall implementation that enforces a subset of the security policy, such as access control, audit, or identification and authentication.
- Security Function Policy (SFP) - the security rules enforced by a security function.

4. Why doesn’t the specification contain requirements for virtual private networking, secure dial-in remote access, etc.?

   Under the philosophy of minimal essential requirements, the protection profile does not address a number of security features, such as those mentioned, since they are needed only by some organizations or appear only in some products. Nevertheless, during an evaluation, laboratories can give credit to products possessing special features, permitting organizations that need them to distinguish among evaluated firewall products. Eventually, as differentiating product features become more widely implemented and used, they may be incorporated into an update of the profile.

5. Why is the specification devoid of detailed, protocol-based filtering requirements?

   The aim of the specification is to define the generic security requirements of a firewall. While most present-day firewalls are primarily or exclusively oriented toward Internet protocols, the protocol filtering requirements in the profile apply equally to firewalls supporting proprietary or non-Internet protocols. Moreover, due to the vast number and ever changing set of protocols in use and under development today, a conscious decision was made to exclude detailed filtering requirements that pertain to protocol specific information contained within headers. During evaluation, protocol specific filtering capabilities claimed by the firewall’s manufacturer are assessed against known vulnerabilities. This approach takes into account both the power that the marketplace bears on the desired capabilities of products, and the ability to conduct security evaluations on an extensive generic class of products.

6. What is the difference between session oriented and non-session oriented services, and why is this distinction being made?

   The underlying notion here is that, generally speaking, there are two classes of firewalls: those that maintain the state of an association between it and another system with regard to identification and authentication, and those that don’t. For example, an application proxy firewall is likely to prompt for a password in response to an attempt to initiate a file transfer protocol exchange from an external source, while a packet filtering firewall is not likely to do so. It is the capability to perform identification and authentication and control subsequent access based on the retention of this information that distinguishes one class of firewall from the other. Since only a few security requirements differ between each class, they are qualified accordingly in a single profile, rather than constructing separate protection profiles.

7. Any guidance on how best to read and interpret the protection profile?

A protection profile should present the reader with a tightly woven view of identified threats, security objectives to counter those threats, functionality that fulfills the security objectives, and assurances needed from an evaluation. Unfortunately, this perspective is not readily apparent, but formulating it from parts of the specification should help improve understanding. In the firewall protection profile, the security objectives identified in section 4 are countermeasures to the threats listed earlier in section 3.3.2. The exact mapping between objectives and threats is given in section 6.1. Similarly, Table 5.1 summarizes the functional security requirements needed to meet the security objectives listed in section 4. The mapping between objectives and requirements is given in section 6.2, which also explains the rationale behind the choices. Table 5.3 summarizes the assurance requirements that are consistent with the threat environment.